

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Smith et al.

Application No.: 10/789,805

Filed: February 27, 2004

For: METHOD AND SYSTEM FOR A  
SERVICE CONSUMER TO CONTROL  
APPLICATIONS THAT BEHAVE  
INCORRECTLY WHEN  
REQUESTING SERVICES

Confirmation No. 5629

Art Unit: 3868

EXAMINER: C.A. Stroder

**APPEAL BRIEF**

MS Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

As required under 37 C.F.R. § 41.37(a), this brief is in furtherance of the Notice of Appeal in this application filed on July 14, 2011. The fees required under 37 C.F.R. § 41.20(b)(2), and any required petition for extension of time for filing this brief and associated fees, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37. The complete Table of Contents follows.

**TABLE OF CONTENTS**

I.	REAL PARTY IN INTEREST .....	1
II.	RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS.....	1
III.	STATUS OF CLAIMS.....	1
IV.	STATUS OF AMENDMENTS.....	1
V.	SUMMARY OF CLAIMED SUBJECT MATTER .....	1
	A. Overview of Appellant's Technology .....	1
	B. Independent Claim on Appeal .....	2
	1. Claim 1 .....	2
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL.....	3
	A. The Examiner's Rejections.....	3
	B. The Issues on Appeal.....	5
	1. Whether the Examiner is impermissibly taking inconsistent positions when rejecting the claims. ....	5
	2. Whether the McCorkendale features that the Examiner asserts correspond to the claim elements are arranged as claimed. ....	5
	3. Whether McCorkendale's client device determines whether the certified software is malicious and then notifies the execution authority.....	5
VII.	ARGUMENTS .....	5
	A. Legal Requirements of Anticipation.....	5
	1. Anticipation .....	5
	2. Obviousness.....	6
	B. The McCorkendale Reference.....	6
	C. Discussion of the Issues (Claims 1, 2, 5, 6, and 9).....	8
	1. The Examiner takes inconsistent positions when rejecting the claims. ....	8
	2. The McCorkendale features that correspond to the claimed elements are not arranged as claimed.....	9

3. McCorkendale's client device does not determine whether a request would exceed the predetermined threshold or notify either the certifying authority or the execution authority that the certified software is misbehaving. .... 10

VIII. CONCLUSION .....	12
CLAIMS APPENDIX .....	13
EVIDENCE APPENDIX .....	15
RELATED PROCEEDINGS APPENDIX .....	16

I. REAL PARTY IN INTEREST

The real party in interest is Microsoft Corporation of Redmond, Washington.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-30 have been presented. Claims 3, 4, 7, 8, and 10-22 have been canceled.<sup>1</sup> The rejection of claims 1, 2, 5, 6, and 9 is being appealed.

IV. STATUS OF AMENDMENTS

Appellant is filing an amendment with this Appeal Brief to cancel claims 10-22.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Overview of Appellant's Technology

Appellant's technology detects when an application that requests services of a service provider is misbehaving in its requesting of services of the service provider. For example, a consumer may want to install a third-party application on the consumer's computer that accesses a server of a stock exchange to provide stock quotes in real time. Because the consumer may not fully trust the application and the fees for the stock quotes may be high, the consumer may want to ensure that the application does not request too many stock quotes. Appellant's technology provides a couple of checks to help prevent an application from misbehaving, such as requesting too many stock quotes.

---

<sup>1</sup> Claims 10-22 were canceled at the time of filing this Appeal Brief.

First, prior to installing the application at a consumer's computer, appellant's technology asks the service provider whether the application is authorized to use the service provider. The service provider may have collected data from other consumers as to the trustworthiness of the application. If the service provider indicates that the application is not authorized, then appellant's technology does not install the application on the consumer's computer. If, however, the service provider indicates that the application is authorized, then appellant's technology installs the application on the consumer's computer.

Second, appellant's technology provides the application with a limit on the services of the service provider that the application is authorized to use based on published requirements of the application. For example, the application may publish that it will not request more than 100 stock quotes per day to put a cap on the fees incurred. During runtime, when the application requests a service of the service provider, a runtime environment at the consumer's computer determines whether the request would exceed the limit. If the request would not exceed the limit, the service provider is requested to provide the service. If, however, the request would exceed the limit, the runtime notifies the service provider that the application is misbehaving and prohibits further execution of the application. Because the application is provided with the limit, an application that is behaving will abide by that limit, while an application that is misbehaving will not.

B. Independent Claim on Appeal

1. Claim 1

The claim is directed to a method in a consumer system with a processor and a memory for determining whether an application is misbehaving. (Spec., ¶ 0030.) When installing an application, the method establishes a limit on the services of a service provider that the application is authorized to use based on published requirements of the application. (Spec., ¶¶ 0009 and 0046.) The service provider is a computer system

that is remote to the consumer system. (Figure 1.) The method asks the service provider whether the application is authorized to use the service provider. (Spec., ¶ 0046, Fig. 12, block 1206.) The service provider determines that the application is not authorized based on notifications received from other consumer systems indicating that the application is misbehaving. (Spec., ¶ 0030.) The method determines whether the application is authorized to request services of the service provider based on a response to the asking of the service provider whether the application is authorized to use the service provider. (Spec., ¶ 0046, Fig. 12, block 1207.) When it is determined that the application is authorized to request services of the service provider, the method installs the application. (Spec., ¶ 0046, Fig. 12, block 1210.) When it is determined that the application is not authorized to request services of the service provider, the method does not install the application. (Spec., ¶ 0046, Fig. 12, block 1208.) Under the control of a runtime environment after the application has been installed, the method provides the application executing on the consumer system with access to an indication of the established limit so that the application can know and abide by the established limit. (Spec., ¶ 0009.) When the application executing on the consumer system requests a service of the service provider, the method determines whether the request would exceed the established limit that is based on published requirements of the application. (Spec., claim 8.) When it is determined that the request would not exceed the established limit, the method requests the service provider to provide the service. (Spec., ¶ 0047, Fig. 13, blocks 1302 and 1304.) When it is determined that the request would exceed the established limit, the method notifies the service provider that the application is misbehaving and prohibits execution of the application on the consumer system. (Spec., ¶ 0047, Fig. 13, blocks 1302, 1305, and 1306.)

## VI. GROUND S OF REJECTION TO BE REVIEWED ON APPEAL

### A. The Examiner's Rejections

The Examiner has rejected claims 1, 5, and 6 under 35 U.S.C. § 102(e) as being anticipated by McCorkendale (U.S. Patent Publication No. 2004/0153644). The

Examiner has also rejected, under 35 U.S.C. § 103(a) as being unpatentable, claim 2 over McCorkendale and Davis (U.S. Patent Publication No. 2003/0135509) and claim 9 over McCorkendale and Choate (U.S. Patent Publication No. 2001/0054026).<sup>2</sup> The Examiner asserts that certain features of McCorkendale correspond to the claim elements as outlined in the following table:

Claim Element	McCorkendale's Feature
service provider	certifying authority <sup>3</sup> execution authority <sup>4</sup>
service	request to certify <sup>5</sup> granting or denial of permission for the software to execute <sup>6</sup>
consumer computer [sic, system]	client device <sup>7</sup>
application	certified software <sup>8</sup>
limit	predetermined threshold <sup>9</sup>

<sup>2</sup> To simplify the issues on appeal, appellant is not separately arguing patentability of the dependent claims. Appellant reserves the right, however, to separately argue the patentability of the dependent claims in subsequent proceedings not directly related to this appeal.

<sup>3</sup> "[C]ertifying authority" is interpreted as the service provider . . . ." Office Action, April 19, 2011, p. 3.

<sup>4</sup> Although the Examiner explicitly states that McCorkendale's certifying authority corresponds to the claimed service provider, the Examiner implicitly also relies on McCorkendale's execution authority as corresponding to the claimed service provider. Id. at p. 6.

<sup>5</sup> "[T]he request to certify the software is interpreted as the 'service' . . . ." Id. at p. 3.

<sup>6</sup> "[T]he service being provided is the granting or denial of permission for the software to execute . . . ." Id. at p. 6.

<sup>7</sup> "[T]he 'client device' is interpreted as the consumer computer . . . ." Id. at p. 4.

<sup>8</sup> Id. at p. 3 (implicitly).

<sup>9</sup> Id. at p. 3 (implicitly).

B. The Issues on Appeal

1. Whether the Examiner is impermissibly taking inconsistent positions when rejecting the claims.
2. Whether the McCorkendale features that the Examiner asserts correspond to the claim elements are arranged as claimed.
3. Whether McCorkendale's client device determines whether the certified software is malicious and then notifies the execution authority.

VII. ARGUMENTS

A. Legal Requirements of Anticipation

1. Anticipation

The Examiner has rejected claims 1, 5, and 6 as being anticipated under 35 U.S.C. § 102(e), which provides:

A person shall be entitled to a patent unless—

....

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent ....

Anticipation requires that each claim element must be identical to a corresponding element in the applied reference. Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc., 45 F.3d 1550, 1554, 33 U.S.P.Q. 2d 1496, 1498 (Fed. Cir. 1995). Indeed, the failure to mention "a claimed element [in] a prior art reference is enough to negate anticipation by that reference." Atlas Powder Co. v. E.I. du Pont De Nemours & Co., 750 F.2d 1569, 1574, 224 U.S.P.Q. 409, 411 (Fed. Cir. 1984). To establish a *prima*



*facie* case of anticipation, the Examiner must identify where "each and every facet of the claimed invention is disclosed in the applied reference." Ex parte Levy, 17 U.S.P.Q.2d 1461, 1462 (Bd. Pat. App. & Interf. 1990). The Federal Circuit has made clear that a "prior art reference—in order to anticipate under 35 U.S.C. § 102—must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements 'arranged as in the claim.'" Net Money!N Inc. v. VeriSign Inc., 545 F.3d 1359, 1369, 88 U.S.P.Q.2d 1751, 1758 (Fed. Cir. 2008) (quoting Connell v. Sears, Roebuck & Co., 722 F.2d 1542, 1548, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983). This requirement applies to all types of claims and refers to the need for a reference to show all limitations of a claim arranged or combined in the same way as recited in the claim, not merely in any particular order. Id.

## 2. Obviousness

The Examiner has rejected claims 2 and 9 as being obvious under 35 U.S.C. § 103(a), which provides:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

### B. The McCorkendale Reference

McCorkendale attempts to detect and prevent malicious software from executing on a client device by detecting whether the software has been tampered with and tracking the frequency at which the software executes at client devices (e.g., a worm will attempt to execute at many client devices). (McCorkendale, Abstract.) Figure 1 of McCorkendale is illustrated below.

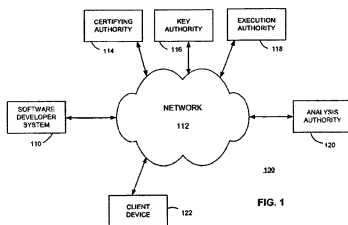


FIG. 1

To detect tampering of software, McCorkendale allows a software developer system 110 to obtain a certification for software from a certifying authority 114. The developer distributes the certification with the software as "certified software." The certification includes a hash of the certified software that is encrypted with the private key of the certifying authority. (McCorkendale, ¶¶ 0008 and 0040-42.) The hash is a numeric value (e.g., 64 bits) that is output by a hash function that is applied to the software. If the certified software is tampered with, the hash function would generate a different hash value (with an extremely high probability). When a client attempts to execute the certified software, the client device 122 generates a hash for the certified software and also decrypts the hash of the certification using the public key of the certifying authority. If the generated hash and the decrypted hash match, then the certified software has not been tampered with and the client device lets the certified software execute. Otherwise, the client device prevents the execution of the tampered-with software. (McCorkendale, ¶ 0069.)

Whenever the client device attempts to execute the certified software, the client device checks for alerts sent by an execution authority 118 that identify that software as malicious. (McCorkendale, ¶¶ 0052 and 0067-68.) The execution authority 118 may identify malicious software based on the number of requests to execute the certified software that have been received from client devices. "An abnormally high number of execution requests within a certain window of time may indicate that the software is a

worm or otherwise malicious." (McCorkendale, ¶ 0068.) The client device permits or denies execution based on whether the execution authority has identified certified software as being malicious.

C. Discussion of the Issues (Claims 1, 2, 5, 6, and 9)

Although McCorkendale and appellant's technology both seek to detect and reduce the impact of malware, they do so in fundamentally different ways. McCorkendale prevents execution of software that is suspected of being tampered with or being malicious. Applicant's technology, in contrast, prevents installation of an application that is not authorized to use a service provider, but if such an application is installed, appellant's technology allows execution of the application and prevents the executing application from accessing the service provider. McCorkendale does not identically disclose the combination of such prevention of installation of an application and such prevention of access during execution of the installed application.

1. The Examiner takes inconsistent positions when rejecting the claims.

In rejecting claim 1, the Examiner states that McCorkendale's "request to certify the software is interpreted as the 'service' of the claims. (Office Action, April 19, 2011, p. 3, emphasis added.) The Examiner then states that "the service being provided is the granting or denial of permission for the software to execute." (Id. at p. 6, emphasis added.) It is inconsistent for the Examiner to take the position that one feature of McCorkendale corresponds to the claimed "service" at one point, and an entirely different feature corresponds to the claimed "service" at another point. The claimed "service" can correspond to either the "request to certify" or the "granting or denial of permission," but it cannot logically correspond to both because the request to certify is performed by the developer during development and the granting or denial is performed by a client device before execution of the software at the client device.

In rejecting the claims, the Examiner states that the "'certifying authority' is interpreted as the service provider." (Id. at p. 3.) The Examiner's arguments also implicitly assume that McCorkendale's execution authority corresponds to the claimed "service provider" because it provides the service of "granting or denial of permission." (Id. at p. 6.) Again, the Examiner's position is inconsistent. It is inconsistent for the certifying authority to correspond to the claimed service provider for some purposes and the execution authority to correspond to the claimed service provider for other purposes, given that the certifying authority and the execution authority are very different. The certifying authority simply provides certification (e.g., encrypted hash) for the software during development, whereas the execution authority determines whether software is malicious based on the number of execution requests.

Because of these inconsistencies in the Examiner's position, the Examiner has not met the burden of pointing out where each and every element of the claim is identically disclosed in McCorkendale and thus has not established a prima facie case of anticipation.

2. The McCorkendale features that correspond to the claimed elements are not arranged as claimed.

Because the Examiner takes contradictory positions as to the correspondences of McCorkendale's features to the claim elements, it is difficult to understand why the Examiner believes that McCorkendale identically discloses each claim element. But even assuming that these inconsistent correspondences were somehow permissible, McCorkendale still would not identically disclose several claim elements as arranged in the claims.

As one example, appellant's claim 1 recites "establishing a limit on services of a service provider that the application is authorized to use." When discussing this language of the claims, the Examiner explicitly states that McCorkendale's "'certifying authority' is interpreted as the service provider and the request to certify the software is

interpreted as the 'service.'" (Office Action, April 19, 2011, p. 3.) The Examiner also relies on the "predetermined threshold" of "software execution frequencies" that are tracked by the McCorkendale's execution authority as corresponding to appellant's limit on services. (*Id.*) McCorkendale's "predetermined threshold" of execution frequencies of software is, however, unrelated to the certification process performed by a developer. A software developer performs the certification long before the certified software is even distributed to client devices, and the "predetermined threshold" is used when the client devices attempt to install or execute certified software after distribution. McCorkendale has nothing to suggest that any limit is placed on requests to certify of a certifying authority. Moreover, McCorkendale's predetermined threshold is not a limit on any services of a service provider; rather, it is a limit on the number of times the certified software can execute before being identified as malicious by the execution authority.

As another example, claim 1 recites "when the application executing on the consumer system requests a service of the service provider." (Emphasis added.) When discussing this language of the claims, the Examiner explicitly states that "the service being provided is the granting or denial of permission for the software to execute." (Office Action, April 19, 2011, p. 6.) McCorkendale's certified software itself, however, never requests "the granting or denial of permission for the software to execute." Rather, McCorkendale's gatekeeper module, which controls the installation and execution of the certified software, determines whether to deny or permit the execution of the certified software. (McCorkendale, ¶¶ 0056-59.) Although McCorkendale's gatekeeper module is software, it is not the potentially malicious certified software that the Examiner asserts corresponds to the claimed "application." Moreover, McCorkendale's certified software (or any other software) cannot itself request permission to execute, because it needs to be already executing to perform any action.

3. McCorkendale's client device does not determine whether a request would exceed the predetermined threshold or notify either

the certifying authority or the execution authority that the certified software is misbehaving.

The claims recite that the consumer system determines "whether the request would exceed the established limit" (i.e., the application is misbehaving), and if so, it notifies "the service provider that the application is misbehaving." In rejecting this claim, the Examiner relies on paragraphs 0049 and 0051 of McCorkendale as describing this notification. (Office Action, April 19, 2011, p. 7.) These relied-upon portions describe the processing of the malicious software detection module 512 and the frequency monitoring module 522 of McCorkendale's execution authority 118. McCorkendale further describes that when the malicious software module identifies malicious software, the broadcast module 524 sends "malicious software" alerts to the client devices. (McCorkendale, ¶ 0052.) McCorkendale's Figure 5, which is reproduced below, illustrates clearly that these three modules are part of the execution authority 118. (See "EXECUTION AUTHORITY" in the lower left corner.)

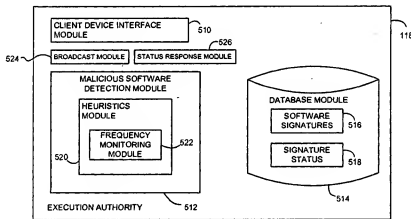


FIG. 5

This is an example of a fundamental difference between McCorkendale and appellant's technology. Appellant's claims recite that the consumer system determines whether the application is misbehaving and, if so, notifies the service provider, whereas in McCorkendale the execution authority identifies the malicious software and sends alerts

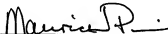
to the client devices. Because McCorkendale's client devices, which the Examiner believes correspond to the claimed consumer system, do not determine whether software is malicious and do not send a notification, McCorkendale does not identically disclose all aspects of the claims as arranged in the claims.

#### VIII. CONCLUSION

Because the Examiner has taken inconsistent positions in rejecting the claims, because McCorkendale's features are not arranged as claimed, and because McCorkendale's client device does not determine whether a request of the executing certified software exceeds the predetermined threshold and does not notify the execution authority of such exceedance, the Examiner has not met his burden of demonstrating that McCorkendale anticipates the claims. As such, appellant respectfully requests that the rejection of claim 1 and its dependent claims be reversed.

DATED: December 9, 2011

PERKINS COIE LLP

By: 

Maurice J. Pirio

Registration No.: 33,273  
1201 Third Avenue, Suite 4800  
Seattle, WA 98101-3099  
Telephone: 206.359.8000  
Facsimile: 206.359.9000

Attorneys for Appellant

**CLAIMS APPENDIX**

Claims Involved in the Appeal of Application Serial No. 10/789,805.

1. A method in a consumer system with a processor and a memory for determining whether an application is misbehaving, the method comprising:
  - when installing an application,
    - establishing a limit on services of a service provider that the application is authorized to use based on published requirements of the application, the service provider being a computer system that is remote to the consumer system;
  - asking the service provider if the application is authorized to use the service provider wherein the service provider determines that the application is not authorized based on notifications received from other consumer systems indicating that the application is misbehaving;
  - determining by the processor whether the application is authorized to request services of the service provider based on a response to the asking of the service provider if the application is authorized to use the service provider;
  - when it is determined that the application is authorized to request services of the service provider, installing the application; and
  - when it is determined that the application is not authorized to request services of the service provider, not installing the application; and
- under control of a runtime environment after the application has been installed,
  - providing the application executing on the consumer system with access to an indication of the established limit so that the application can know and abide by the established limit;



when the application executing on the consumer system requests a service of the service provider,  
determining by the processor whether the request would exceed the established limit that is based on published requirements of the application;  
when it is determined that the request would not exceed the established limit, requesting the service provider to provide the service; and  
when it is determined that the request would exceed the established limit,  
notifying the service provider that the application is misbehaving; and  
prohibiting execution of the application on the consumer system.

2. The method of claim 1 wherein the prohibiting includes uninstalling the application.

5. The method of claim 1 wherein the service provider aggregates notifications provided by different consumer systems to determine whether the application should be authorized to request services of the service provider.

6. The method of claim 1 wherein the service provider aggregates notifications provided by the consumer system to determine whether the consumer system should not be authorized to request services of the service provider.

9. The method of claim 1 wherein multiple service providers can provide equivalent services and the application can request services one of those service providers as designated by the consumer system.

**EVIDENCE APPENDIX**

No evidence pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Examiner is being submitted.

**RELATED PROCEEDINGS APPENDIX**

No related proceedings are referenced in Section II.; hence copies of decisions in related proceedings are not provided.